

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-326693
 (43)Date of publication of application : 22.11.2001

(51)Int.Cl. H04L 12/66
 H04L 12/56
 H04L 12/22

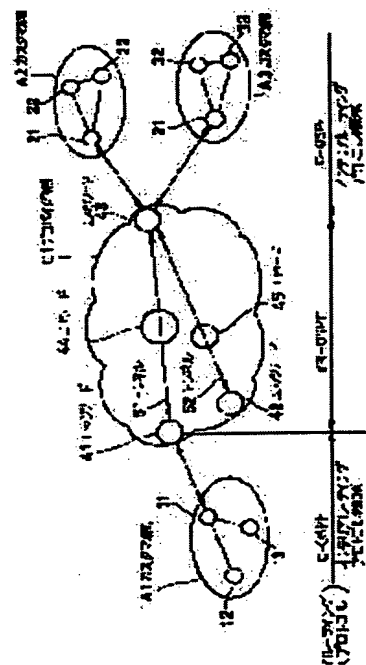
(21)Application number : 2000-144234 (71)Applicant : NEC CORP
 (22)Date of filing : 17.05.2000 (72)Inventor : KAWAKAMI HIROYUKI

(54) COMMUNICATION SYSTEM AND METHOD FOR CONTROLLING COMMUNICATION, AND CONTROL PROGRAM RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a communication unit in which the installation of a BGP is not required for a customer communication unit and for an edge communication unit at a border between a customer network and a provider network, to prevent a load from being increased and, to provide a communication system that uses the communication unit.

SOLUTION: In a virtual private network(VPN), consisting of customer networks A1-A4 and a provider network C1 utilizing tunneling technology, a function for terminating IGP(Interior Gateway Protocols) in the customer networks is provided to edge nodes 41-43 placed at the border between the customer networks and the provider network. Thus, the installation of the BGP(Border Gateway Protocol) is not required with respect to customer nodes and to the edge nodes, at the border between the customer networks and the provider network.



LEGAL STATUS

[Date of request for examination] 13.04.2001

[Date of sending the examiner's decision of rejection] 12.10.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

BEST AVAILABLE COPY

decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-326693

(P2001-326693A)

(43) 公開日 平成13年11月22日 (2001. 11. 22)

(51) Int.Cl. ⁷	識別記号	F I	テームト* (参考)
H 0 4 L 12/66		H 0 4 L 11/20	B 5 K 0 3 0
12/56			1 0 2 A
12/22		11/26	

審査請求 有 請求項の数25 O L (全 14 頁)

(21) 出願番号 特願2000-144234(P2000-144234)

(22) 出願日 平成12年5月17日 (2000. 5. 17)

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 川上 弘幸

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100088812

弁理士 ▲柳▼川 信

Fターム(参考) 5K030 GA04 GA11 HA08 HCD1 HD03
HD06 LA08 LB20

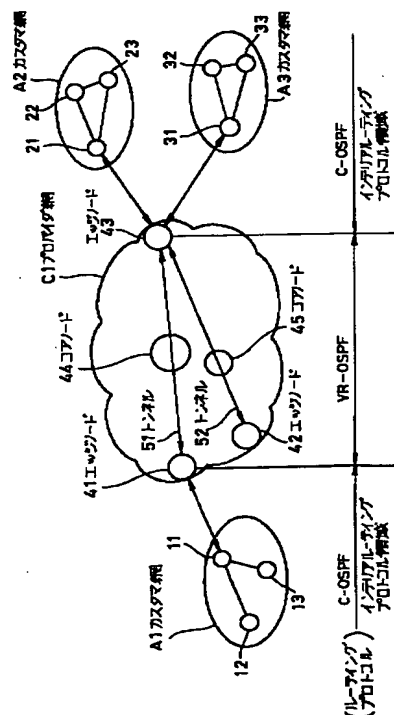
(54) 【発明の名称】 通信装置及び通信制御方法並びに制御プログラム記録媒体

(57) 【要約】

【課題】 カスタマ網とプロバイダ網との境界においてカスタマ通信装置とエッジ通信装置とに対してBGPの実装を不要として、負荷の増大を防止した通信装置及びそれを使用した通信システムを得る。

【解決手段】 複数のカスタマ網A1～A3と、トンネル化技術を利用したプロバイダ網C1からなるVPNにおいて、カスタマ網とプロバイダ網との境界に位置するエッジノード41～43に、カスタマ網内のIGPs

(Interior Gateway Protocols) を終端する機能を設ける。これにより、カスタマ網とプロバイダ網との境界においてカスタマノードとエッジノードとに対して、BGP (Border Gateway Protocol) の実装が不要となる。



【特許請求の範囲】

【請求項 1】 プロバイダ網上にトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線（VPN）を構築するようにした通信システムにおいて、前記トンネルの入出力端に接続されたエッジ通信装置であって、前記カスタマ網内で使用されるルーティングプロトコルを終端する終端手段を含むことを特徴とするエッジ通信装置。

【請求項 2】 前記仮想専用線に関する VPN 構築情報と、前記プロバイダ網に接続され予めカプセルアドレスが割り当てられたポートと前記カスタマ網側の各通信装置の IP アドレスとの対応情報とからなるテーブルを更に含み、

前記終端手段は、前記カスタマ網から入力されたパケットの宛先アドレスから前記テーブルを検索する検索手段と、この検索されたカプセルアドレスを基に前記パケットをカプセル化して前記プロバイダ網へ送出するカプセル化手段とを有することを特徴とする請求項 1 記載のエッジ通信装置。

【請求項 3】 前記カプセル化手段は、同一の仮想専用線に属する他のカスタマ網に対して、前記カプセルアドレスを基に前記制御パケットをカプセル化して送出するようにしたことを特徴とする請求項 2 記載のエッジ通信装置。

【請求項 4】 前記終端手段は、前記カスタマ網内の IP アドレスの追加やトポロジの変化にตอบสนองして前記カスタマ網で生成される制御パケットを受信解読する手段と、この解読結果に従って前記テーブルのデータ更新を行う手段とを有することを特徴とする請求項 2 または 3 記載のエッジ通信装置。

【請求項 5】 前記終端手段は、前記プロバイダ網から自装置に到着したパケットに対して前記カプセルアドレスが含まれるカプセルを外し、当該パケットに含まれる宛先 IP アドレスを基に前記テーブルから送出先を決定して送出する手段を有することを特徴とする請求項 2～4 いずれか記載のエッジ通信装置。

【請求項 6】 前記終端手段は、前記カスタマ網に対する現用インタフェースの障害にตอบสนองしてこの障害インタフェースに関連する前記テーブル内の情報を削除すると共に、関連する他のエッジ通信装置へ障害通知及び予備インタフェースの通知をなす手段を有することを特徴とする請求項 2～5 いずれか記載のエッジ通信装置。

【請求項 7】 前記終端手段は、他のエッジ通信装置からの障害通知にตอบสนองして前記障害インタフェースに関連する前記テーブル内の情報を削除すると共に、前記予備インタフェースの通知にตอบสนองして前記テーブル内にこの予備インタフェースに関連する情報を追加する手段を有することを特徴とする請求項 6 記載のエッジ通信装置。

【請求項 8】 前記カスタマ網内で使用されるルーティングプロトコルは、OSPF（Open Shortest Path Fir

st）プロトコルであることを特徴とする請求項 1～7 いずれか記載のエッジ通信装置。

【請求項 9】 プロバイダ網上におけるエッジ通信装置間にてトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線（VPN）を構築するようにした通信システムにおける通信制御方法であって、前記エッジ通信装置において、前記カスタマ網内で使用されるルーティングプロトコルを終端する終端ステップを含むことを特徴とする通信制御方法。

【請求項 10】 前記エッジ通信装置には、前記仮想専用線に関する VPN 構築情報と、前記プロバイダ網に接続され予めカプセルアドレスが割り当てられたポートと前記カスタマ網側の各通信装置の IP アドレスとの対応情報とからなるテーブルが設けられており、

前記終端ステップは、前記カスタマ網から入力されたパケットの宛先アドレスから前記テーブルを検索する検索ステップと、この検索されたカプセルアドレスを基に前記パケットをカプセル化して前記プロバイダ網へ送出するカプセル化ステップとを有することを特徴とする請求項 9 記載の通信制御方法。

【請求項 11】 前記カプセル化ステップは、同一の仮想専用線に属する他のカスタマ網に対して前記カプセルアドレスを基に前記制御パケットをカプセル化して送出するようにしたことを特徴とする請求項 10 記載の通信制御方法。

【請求項 12】 前記終端ステップは、前記プロバイダ網から自装置に到着したパケットに対して前記カプセルアドレスが含まれるカプセルを外し、当該パケットに含まれる宛先 IP アドレスを基に前記テーブルから送出先を決定して送出するステップを有することを特徴とする請求項 10 または 11 記載の通信制御方法。

【請求項 13】 前記終端ステップは、前記カスタマ網内の IP アドレスの追加やトポロジの変化にตอบสนองして前記カスタマ網で生成される制御パケットを受信解読するステップと、この解読結果に従って前記テーブルのデータ更新を行うステップとを有することを特徴とする請求項 10～12 いずれか記載の通信制御方法。

【請求項 14】 前記終端ステップは、前記カスタマ網との現用インタフェースの障害にตอบสนองしてこの障害インタフェースに関連する前記テーブル内の情報を削除すると共に、関連する他のエッジ通信装置へ障害通知及び予備インタフェースの通知をなすステップを有することを特徴とする請求項 10～13 いずれか記載の通信制御方法。

【請求項 15】 前記終端ステップは、他のエッジ通信装置からの障害通知にตอบสนองして前記障害インタフェースに関連する前記テーブル内の情報を削除すると共に、前記予備インタフェースの通知にตอบสนองして前記テーブル内にこの予備インタフェースに関連する情報を追加するステップを有することを特徴とする請求項 14 記載の通信

制御方法。

【請求項16】 前記カスタマ網内で使用されるルーティングプロトコルは、OSPF (Open Shortest Path First) プロトコルであることを特徴とする請求項9～15いずれか記載の通信制御方法。

【請求項17】 前記テーブルを集中管理する集中処理装置が設けられており、前記制御パケットの解釈結果に従って前記テーブルのデータ更新後に、この更新されたテーブルを前記集中処理装置へアップロードするステップと、前記集中処理装置からこのアップロードされたテーブルに関連するエッジ通信装置にダウンロードするステップとを含むことを特徴とする請求項13記載の通信制御方法。

【請求項18】 プロバイダ網上におけるエッジ通信装置間にてトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線 (VPN) を構築するようにした通信システムにおける通信制御方法のプログラムを記録した記録媒体であって、前記プログラムは、前記エッジ通信装置において、前記カスタマ網内で使用されるルーティングプロトコルを終端する終端ステップを含むことを特徴とする記録媒体。

【請求項19】 前記エッジ通信装置には、前記仮想専用線に関するVPN構築情報と、前記プロバイダ網に接続され予めカプセルアドレスが割り当てられたポートと前記カスタマ網側の各通信装置のIPアドレスとの対応情報とからなるテーブルが設けられており、前記終端ステップは、前記カスタマ網から入力されたパケットの宛先アドレスから前記テーブルを検索する検索ステップと、この検索されたカプセルアドレスを基に前記パケットをカプセル化して前記プロバイダ網へ送出するカプセル化ステップとを有することを特徴とする請求項18記載の記録媒体。

【請求項20】 前記カプセル化ステップは、同一の仮想専用線に属する他のカスタマ網に対して前記カプセルアドレスを基に前記制御パケットをカプセル化して送出するようにしたことを特徴とする請求項19記載の記録媒体。

【請求項21】 前記終端ステップは、前記プロバイダ網から自装置に到着したパケットに対して前記カプセルアドレスが含まれるカプセルを外し、当該パケットに含まれる宛先IPアドレスを基に前記テーブルから送出先を決定して送出するステップを有することを特徴とする請求項19または20記載の記録媒体。

【請求項22】 前記終端ステップは、前記カスタマ網内のIPアドレスの追加やトポロジの変化にตอบสนองして前記カスタマ網で生成される制御パケットを受信解釈するステップと、この解釈結果に従って前記テーブルのデータ更新を行うステップとを有することを特徴とする請求項19～21いずれか記載の記録媒体。

【請求項23】 前記終端ステップは、前記カスタマ網

に対する現用インタフェースの障害にตอบสนองしてこの障害インタフェースに関連する前記テーブル内の情報を削除すると共に、関連する他のエッジ通信装置へ障害通知及び予備インタフェースの通知をなすステップを有することを特徴とする請求項19～22いずれか記載の記録媒体。

【請求項24】 前記終端ステップは、他のエッジ通信装置からの障害通知にตอบสนองして前記障害インタフェースに関連する前記テーブル内の情報を削除すると共に、前記予備インタフェースの通知にตอบสนองして前記テーブル内にこの予備インタフェースに関連する情報を追加するステップを有することを特徴とする請求項23記載の記録媒体。

【請求項25】 前記カスタマ網内で使用されるルーティングプロトコルは、OSPF (Open Shortest Path First) プロトコルであることを特徴とする請求項18～24いずれか記載の記録媒体。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は通信装置及び通信制御方法並びに制御プログラム記録媒体に関し、特にプロバイダ網上にトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線 (VPN) を構築するようにした通信方式に関するものである。

【0002】

【従来の技術】 カプセル化技術を用いたVPN (Virtual Private Network) 構築技術に関して、シスコ (Cisco) 社から、プロバイダ網にMPLS (Multi Protocol Label Switch) を用いた通信方式が提案されている。この様なVPN技術について説明する。VPNとは、インターネット等の公衆通信網上で、論理的なグループを形成し、かつそのグループ間で閉域性を保つ機能を設けたネットワークをいう。このインターネット等の公衆通信網には、通常不特定多数のユーザが接続しており、そのために基本的には特定のユーザだけの通信はできず、第三者による不正アクセスは避けられないというセキュリティ上の問題がある。

【0003】 そこで、近年エンドーエンドでセキュリティ対策を施すことにより、インターネット上に仮想的に専用線を構築し、LAN (Local Area Network) 間接続の基幹回線として利用するVPN技術が注目されている。具体的には、エンドーエンドでのデータの暗号化、ユーザ認証及びアクセス制御等のセキュリティを施した上で、特定の拠点間をインターネットを介して接続し、閉域性のあるグループを提供するものである。

【0004】 かかるVPNを公衆通信網上に実現することで、特定ユーザだけの通信が可能となり、インターネット等を仮想的な専用網として利用することができるのである。この様なVPN方式に関しては、特開平10-70566号公報、特開平11-355272号公報等

に開示のものがある。

【0005】図16はこの様なVPNを使用した通信システムの概略ブロック図である。図16において、LAN等の閉域性のあるグループであるカスタマ網A1～A3と、インターネット等のプロバイダ網C1とがある。カスタマ網A1はカスタマ通信装置（以下、通信装置のことを単にノードと称する）11～13を有しており、また、カスタマ網A2はカスタマノード21～23を有しており、更にカスタマ網A3はカスタマノード31～33を有している。そして、プロバイダ網C1には、カスタマ網との境界にエッジノード41～43が設けられており、境界以外にはコアノード44、45が設けられている。尚、図16では、カスタマ網A1との境界にエッジノード41が、カスタマ網A2、A3との境界にエッジノード42が、それぞれ設けられているものとす

る。

【0006】この場合、カスタマ網A1とA2、A3との間の通信は、エッジノード間に構築されたトンネル51により形成されたVPNによって行われるが、このときのルーティングのためのプロトコルの関係は図示のようになっている。すなわち、LAN等のカスタマ網A1～A3では、インテリアルルーティングプロトコルであるIGP（Interior Gateway Protocol）が用いられ、プロバイダ網C1では、IBGP（Interior Border Gateway Protocol）が用いられ、これ等網間のインタフェース部分では、EBGP（Exterior Border Gateway Protocol）が用いられる。

【0007】

【発明が解決しようとする課題】従来のVPN通信方式の問題点としては、図16に示したLAN等の閉域性のあるグループであるカスタマ網A1～A3と、インターネット等のプロバイダ網C1との境界では、EBGPが使用されているので、カスタマノードとエッジノードとに対してBGP（Border Gateway Protocol）による通信ができるように設定する必要がある。これは、カスタマノードにBGPを実装する必要があるばかりではなく、サービスを受けるカスタマがBGPの知識が必要となり、負荷の増大を招くという欠点がある。

【0008】また、このようなVPN方式では、カスタマ網とプロバイダ網との境界でEBGPが使用されているので、カスタマ網とプロバイダ網との間で、いわゆるマルチホーミング構成を構築することができない。従って、例えば、帰属するエッジノードが停止した場合や、帰属するインタフェース部分にリンク断が生じた場合には、配下のカスタマ網の通信停止を引き起こし、信頼性の低下につながるという欠点がある。

【0009】更に、プロバイダ網であるMPLS網をプロバイダ網C1内部でVPN毎の経路情報がBGPで伝達されるので、カスタマ網内で使用されるルーティングプロトコルであるOSPF（Open Shortest Path First）

t)のOSPF情報が透過的に通らず、結果としてOSPFドメインが分断されることになる。特に、ATM（非同期通信モード）やFR（フレームリレー）を使用した専用線上でIP網を構築する方式のように、単一のOSPFドメインで各カスタマ網を接続する重要性は極めて大きいにもかかわらず、図16の方式では、OSPFドメインが分断されてしまうので、単一のOSPFドメインで各カスタマ網を接続することができないという欠点もある。

【0010】本発明の目的は、カスタマ網とプロバイダ網との境界においてカスタマノードとエッジノードとに対してBGPの実装を不要として、負荷の増大を防止した通信装置及び通信制御方法並びにその制御プログラムの記録媒体を提供することである。

【0011】本発明の他の目的は、カスタマ網とプロバイダ網との間でのマルチホーミングを構築可能として、信頼性の向上を図った通信装置及び通信制御方法並びにその制御プログラムの記録媒体を提供することである。

【0012】本発明の更に他の目的は、OSPFドメインが分断されてしまうことをなくして、単一のOSPFドメインで各カスタマ網を接続することが可能な通信装置及び通信制御方法並びにその制御プログラムの記録媒体を提供することである。

【0013】

【課題を解決するための手段】本発明によれば、プロバイダ網上にトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線（VPN）を構築するようにした通信システムにおいて、前記トンネルの入出力端に接続されたエッジ通信装置であって、前記カスタマ網内で使用されるルーティングプロトコルを終端する終端手段を含むことを特徴とするエッジ通信装置が得られる。

【0014】そして、前記仮想専用線に関するVPN構築情報と、前記プロバイダ網に接続され予めカプセルアドレスが割り当てられたポートと前記カスタマ網側の各通信装置のIPアドレスとの対応情報とからなるテーブルを更に含み、前記終端手段は、前記カスタマ網から入力されたパケットの宛先アドレスから前記テーブルを検索する検索手段と、この検索されたカプセルアドレスを基に前記パケットをカプセル化して前記プロバイダ網へ送出するカプセル化手段とを有することを特徴とする。

【0015】また、前記終端手段は、前記カスタマ網内のIPアドレスの追加やトポロジの変化にตอบสนองして前記カスタマ網で生成される制御パケットを受信解読する手段と、この解読結果に従って前記テーブルのデータ更新を行う手段とを有することを特徴とし、前記カプセル化手段は、同一の仮想専用線に属する他のカスタマ網に対して、前記カプセルアドレスを基に前記制御パケットをカプセル化して送出するようにしたことを特徴とする。

【0016】更に、前記終端手段は、前記プロバイダ網

から自装置に到着したパケットに対して前記カプセルアドレスが含まれるカプセルを外し、当該パケットに含まれる宛先 IP アドレスを基に前記テーブルから送出先を決定して送出する手段を有することを特徴とし、また前記終端手段は、前記カスタマ網に対する現用インタフェースの障害にตอบสนองしてこの障害インタフェースに関連する前記テーブル内の情報を削除すると共に、関連する他のエッジ通信装置へ障害通知及び予備インタフェースの通知をなす手段を有することを特徴とする。

【0017】更にはまた、前記終端手段は、他のエッジ通信装置からの障害通知にตอบสนองして前記障害インタフェースに関連する前記テーブル内の情報を削除すると共に、前記予備インタフェースの通知にตอบสนองして前記テーブル内にこの予備インタフェースに関連する情報を追加する手段を有することを特徴とし、前記カスタマ網内で使用されるルーティングプロトコルは、OSPF プロトコルであることを特徴とする。

【0018】本発明によれば、プロバイダ網上におけるエッジ通信装置間にてトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線（VPN）を構築するようにした通信システムにおける通信制御方法であって、前記エッジ通信装置において、前記カスタマ網内で使用されるルーティングプロトコルを終端する終端ステップを含むことを特徴とする通信制御方法が得られる。

【0019】そして、前記エッジ通信装置には、前記仮想専用線に関する VPN 構築情報と、前記プロバイダ網に接続され予めカプセルアドレスが割り当てられたポートと前記カスタマ網側の各通信装置の IP アドレスとの対応情報とからなるテーブルが設けられており、前記終端ステップは、前記カスタマ網から入力されたパケットの宛先アドレスから前記テーブルを検索する検索ステップと、この検索されたカプセルアドレスを基に前記パケットをカプセル化して前記プロバイダ網へ送出するカプセル化ステップとを有することを特徴とする。

【0020】また、前記終端ステップは、前記カスタマ網内の IP アドレスの追加やトポロジの変化にตอบสนองして前記カスタマ網で生成される制御パケットを受信解読するステップと、この解読結果に従って前記テーブルのデータ更新を行うステップとを有することを特徴とし、更に前記カプセル化ステップは、同一の仮想専用線に属する他のカスタマ網に対して前記カプセルアドレスを基に前記制御パケットをカプセル化して送出するようにしたことを特徴とする。

【0021】更にはまた、前記終端ステップは、前記プロバイダ網から自装置に到着したパケットに対して前記カプセルアドレスが含まれるカプセルを外し、当該パケットに含まれる宛先 IP アドレスを基に前記テーブルから送出先を決定して送出するステップを有することを特徴とし、また前記終端ステップは、前記カスタマ網との

現用インタフェースの障害にตอบสนองしてこの障害インタフェースに関連する前記テーブル内の情報を削除すると共に、関連する他のエッジ通信装置へ障害通知及び予備インタフェースの通知をなすステップを有することを特徴とする。

【0022】更に、前記終端ステップは、他のエッジ通信装置からの障害通知にตอบสนองして前記障害インタフェースに関連する前記テーブル内の情報を削除すると共に、前記予備インタフェースの通知にตอบสนองして前記テーブル内にこの予備インタフェースに関連する情報を追加するステップを有することを特徴とする。また、前記テーブルを集中管理する集中処理装置が設けられており、前記制御パケットの解読結果に従って前記テーブルのデータ更新後に、この更新されたテーブルを前記集中処理装置へアップロードするステップと、前記集中処理装置からこのアップロードされたテーブルに関連するエッジ通信装置にダウンロードするステップとを含むことを特徴とする。

【0023】本発明によれば、プロバイダ網上におけるエッジ通信装置間にてトンネルを形成することにより、複数のカスタマ網間の通信のための仮想専用線（VPN）を構築するようにした通信システムにおける通信制御方法のプログラムを記録した記録媒体であって、前記プログラムは、前記エッジ通信装置において、前記カスタマ網内で使用されるルーティングプロトコルを終端する終端ステップを含むことを特徴とする記録媒体が得られる。

【0024】本発明の作用を述べる。プロバイダ網とカスタマ網との境界に位置するエッジ通信装置において、カスタマ網でのルーティングプロトコルを終端する構成とする。これにより、カスタマ網とプロバイダ網との境界においてカスタマ通信装置とエッジ通信装置とに対して BGP の実装を不要として、負荷の増大を防止し、またカスタマ網のルーティングプロトコルとして、OSPF プロトコルを使用することで、プロバイダ網との間でのマルチホーミングを構築可能となり、信頼性の向上が図れる。更に、単一 OSPF ドメインで各カスタマ網を接続することが可能となるものである。

【0025】

【発明の実施の形態】以下に、図面を参照しつつ本発明の実施の形態につき詳述する。図 1 は本発明によるエッジノードを用いて構築した VPN 構成を説明するための概略システム構成図であり、図 16 と同等部分は同一符号により示している。ここで提案される VPN 構築方式は、カスタマノード 11～13、21～23、31～33 からなるカスタマ網 A1～A3 と、コアノード 44、45 とエッジノード 41～43 とからなるプロバイダ網 C1 とにより構成されている。

【0026】図 1 におけるカスタマ網 A1、カスタマ網 A2、カスタマ網 A3 は、プロバイダ網 C1 の境界で

の、すなわちトンネル51や52の両端に位置するエッジノードでのカプセル化処理によるトンネリングにより、VPNを構築している。従って、カスタマ網A1～A3は同一のAS (Autonomous System) に属し、同一のIGPs (Interior Gateway Protocols)、例えば、RIP (Routing Information Protocol)、OSPF (Open Shortest Path First) により、カスタマノードのトポロジデータベースを更新/管理することができる。尚、本例では、IGPsとしてOSPFを使用するものとしている。

【0027】エッジノード41～43の各々のカスタマ網側は、接続されたカスタマ網で使われているOSPFプロトコルの終端処理が可能であり、よって図1に示すように、カスタマ網A1～A3はC (Customer) - OSPFが使用可能であり、プロバイダ網C1はVR (VPN ROUTING) - OSPFが使用可能であり、図13に示したようにカスタマ網とプロバイダ網との間のインタフェース部で使用されていたEBGPを使用する必要がなくなる。すなわち、カスタマ網側のC-OSPF制御パケットは、プロバイダ網内では、一般のIPパケットとして転送され、トンネルとなるのである。各C-OSPFはプロバイダ網内のVR-OSPFの存在に気付かないということであり、つまりは、各C-OSPFは同じOSPFドメインに属することになる。これ等を実現する機能として、エッジノードにおいて、終端機能とVRテーブル情報の更新機能とを設けるものである。

【0028】また、OSPFでは、複数のリンクに対して異なるメトリック値を設定しておき、メトリック値が、例えば小なるリンクを優先的に選択する、いわゆるマルチホーミングが使用可能であるので、カスタマ網とプロバイダ網との間でこのマルチホーミングを構築可能として、信頼性の向上を図り得るのである。

【0029】図2は本発明の実施例を示すシステム概略図であり、図1と同等部分は同一符号にて示している。尚、図2では、簡単化のためにコアノードは省略して示している。図2に示すように、カスタマ網A1のカスタマノード11～13のプライベートIP (Internet Protocol) アドレスは“aa”、“ab”、“ac”とし、またカスタマ網A2のカスタマノード21～23のプライベートIPアドレスは“ba”、“bb”、“bc”とし、更にカスタマ網A3のカスタマノード31～33のプライベートIPアドレスは“ca”、“cb”、“cc”とする。

【0030】エッジノード41～43のプロバイダ網C1側のカプセルアドレスは“E1”～“E3”とする。そして、エッジノード41のカスタマ網側のインタフェースのアドレス (プライベートIPアドレス) は“11”とし、エッジノード42のカスタマ網側のインタフェースのIPアドレスは“12”とし、エッジノード43のカスタマ網側のインタフェースのIPアドレスは

“13”及び“132”とする。

【0031】そして、本実施例では、前述のマルチホーミングのためのカスタマ網A1内でのトポロジデータベース (ルーティングのためのルーティングテーブル) に対して、2つのプライベートIPアドレス“11”と“12”とを、予め提供しておくものとする。カスタマ網A1内でのルーティングプロトコル (OSPF) において、この提供された2つのIPアドレス“11”、“12”を経路とするメトリック値の大小を、前者の経路の値がより小となるようにしておくことで、IPアドレス“11”を経るルーティングであるVPNトンネル51が現用系として選択されるようにすることができる。

【0032】図3は図2におけるエッジノードの概略ブロック図であり、カスタマ網からのパケットを終端処理する終端部1と、この終端部の動作制御やルーティングの制御をなす制御部 (CPU) 2と、VPN構築情報及びプロバイダ網に接続され予めカプセルアドレスが割り当てられたポートとカスタマ網の各ノードのIPアドレスとの対応情報を有するテーブル、すなわちVRテーブル3と、制御部の動作制御プログラム (ソフトウェア) を予め格納したROM4と、カスタマ網及びプロバイダ網とのインタフェースをなすI/F部5、6とを有している。

【0033】図4はエッジノード41～43が夫々有するルーティング制御のためのVRテーブルの概念図を示しており、VRテーブルは同じVPN ID (VPN識別情報) を持ってもそれが格納されるエッジノードによりその内容は相違しており、図4に示すように、エッジノード41はVR IDとして“11”、“12”、“13”、……に夫々対応するVRテーブルを有しており、VR ID“11”の具体例 (図2に対応) が図5に示されている。また、エッジノード42はVR IDとして“21”、“22”、“23”、……に夫々対応するVRテーブルを有しており、VR ID“21”の具体例 (図2に対応) が図6に示されている。更に、エッジノード43はVR IDとして“31”、“32”、“33”、……に夫々対応するVRテーブルを有しており、VR ID“31”の具体例 (図2に対応) が図7に示されている。

【0034】これ等VRテーブルはカスタマ網側インタフェース (INF) の関連付け情報を含んでおり、これはIP-VPNサービスをプロバイダ網に申し込む際に登録されるもので、カスタマ網側でプライベートアドレスが使用できるようにするための不可欠な情報である。

(異なるカスタマ網で同じアドレスが存在し得る場合があり、この場合どのカスタマ網側インタフェースから入力されてきたかでVRテーブルを識別するものである)。また、Egress (出力) エッジノードのカスタマ側インタフェースの状態、つまりそのカプセル化ア

ドレスが有効であるかどうかの情報(OK/NG)をも含んでいる。

【0035】更に、VPN IDをも含んでいる。このVPN IDはそのVRテーブルを使用するカスタマに付与されたグローバルユニークな情報である。VRテーブルは同じVPN IDを持っていたり、それが格納されるエッジノードにより相違するものである(図4参照)。また、カプセル化アドレスの優先度を含み、この優先度は先述したメトリック値に相当するものであって、優先度“1”(現用系)が“2”(予備系)よりも優先するものとする。

【0036】図8は本発明の実施例の動作を示すシーケンス図であり、カスタマ網からのパケット転送時と、カスタマ網でのアドレス変更時と、メトリック小(現用系)のリンク断時との、各場合におけるものである。先ず、カスタマ網からのパケット転送時について、図9のフローチャートをも参照しつつ説明する。例えば、カスタマ網A1のノード12から他のカスタマ網A2のノード22へパケット転送要求があるとする(ステップS1)。このときのパケットは、図10(A)に示すように、そのヘッダ部分に、送信元アドレス/宛先アドレスとして、a b / b b が表記されている。

【0037】カスタマ網A1内でのOSPFルーティングプロトコルに従って当該パケットはノード11を経て、メトリック値が小のリンクが自動的に選択されてエッジノード41へ供給される。エッジノード41では、終端処理が行われる。すなわち、そのパケットの転送先を解決すべく、先ずこのパケットが入力されてきたカスタマ網側インタフェースI11から定まるVRテーブル(11)を得る(ステップS2)。このVRテーブル(11)から網内パケットに含ませるべきVPN ID(1)を得る(ステップS3)。

【0038】次に、宛先プライベートアドレス(b b)と、Egressエッジノードのカスタマ側INF状態(OK)を元に、カプセル化アドレス(E3)を解決し(ステップS4)、図10(B)に示すように、VPN IDと送信元カプセル化アドレス/宛先カプセル化アドレスであるE1/E3とがヘッダに付加されて、カプセル化が行われる(ステップS5)。このカプセル化されたパケットは対応する出力INF(プロバイダ網側)へ網内パケットとして転送される(ステップS6)。

【0039】このカプセルを受信したエッジノード43での動作を図11のフローチャートに示している。エッジノード43では、このカプセルを終端部1で受信して(ステップS11)、当該網内パケット転送先を解決するために、先ず当該パケットが持つVPN IDを元に、VRテーブル(31)を得て、このVRテーブル(31)内で、宛先プライベートIPアドレス(b b)を元に、対応する出力INF(I31)を決定する(ステップS12)。そして、図10(C)に示すように、

カプセル化アドレスとVPN IDとをヘッダから外して逆カプセル化を行い(ステップS14)、送信する(ステップS15)。

【0040】カスタマ網内のアドレスが変更された場合の動作を、図12のフローチャートを参照して説明する。あるカスタマ網のあるノードのIPアドレスが変更になると、その変更を通知するための制御パケットが網内で転送され(Helloプロトコル等を使用して)、対応するエッジノードにも送信される(ステップS21)。

【0041】この制御パケットのヘッダ部には、このパケットが制御パケットである旨を示す情報が予め付加されているので、この情報により終端部1は制御パケットの認識が可能であり、この制御パケットにのせられているアドレス変更の情報を解釈して、VRテーブルの内容の更新を行う(ステップS22)。そして、プロバイダ網内におけるVRテーブルの情報の交換をなすための交換プロトコルを使用して、関連するエッジノードに対して、アドレス変更の通知を行う(ステップS23)。

【0042】現用トンネルに対応するインタフェースのリンク(メトリック値が小)が断となった場合における動作を、図13のフローチャートを使用して説明する。図2に示したメトリック値が小のリンクが断になると、その障害を通知するための制御パケットが網内で転送される(Helloプロトコル等を使用して)ので、各カスタマノードでは、トポロジDB(データベース)が更新される。

【0043】このとき、障害リンクに接続されているエッジノード41では、障害発生が検出され(ステップS31)、VRテーブルから断リンクに関連する情報が削除される(ステップS32)。この場合の削除の方法としては、VRテーブル内のEgress側のカスタマ網INF状態が、NGに設定されることでなされる。これにより、トンネル51に関する情報はテーブルから削除されたことと等価になる。そして、交換プロトコルにより関連するエッジノードに対して同様に削除通知の他に、メトリックの小なるリンクがアクティブになる旨の通知がなされる(ステップS33)。

【0044】次に、図14のフローチャートを参照すると、図11のステップS33による通知を受けた場合(ステップS41)、そのVRテーブルから断リンクに関する情報が削除される(ステップS42)。同時に、メトリックの大なるリンクがアクティブになる旨の通知により、VRテーブルに対して、このメトリックの大のリンクに関する情報が追加される(ステップS43)。

【0045】ここで、IGPsとしてOSPFを想定した場合、現用系として使用したいエッジ通信網に対してメトリック値を小さく設定し、他方のメトリック値は大きく設定しておく(VPNのメトリック値には、プロバイダ網内の経路を反映する方式と、しない方式とが考えられるが、ここでは、プロバイダ網内の経路から算出さ

れるメトリック値はVPNのメトリック値に反映しないこととする。従って、図2の様なマルチホーミング構成では、メトリック値に大差をつける必要はなく、大小の関係が成立すればよい。

【0046】カスタマ網内のアドレスやトポロジの変更に伴うVRテーブルの更新には、プロバイダ網内でIBGPを使う前述した方式と、集中型処理装置を介して更新する方式とが考えられる。図15はこの集中型処理装置を使用した方式の例であり、図2と同等部分は同一符号にて示している。この例では、集中処理装置100が一方のエッジノードからVPN構築情報をアップロードし、しかる後に関係するエッジノード内VRテーブルにダウンロードすることが考えられる。

【0047】

【発明の効果】本発明によれば、カスタマノードは、BGPをサポートする必要はなく、IGPのみでVPNが構築できるという効果がある。また、カスタマノードが複数のエッジノードに接続されるマルチホーミング構成を、BGPを使用することなく構成することができ、VPNの信頼性を向上させることができるという効果もある。更に、OSPFドメインの分断がなくなり、ATMやFRを使用した専用線上でIP網を構築する方式のように、単一OSPFドメインで、各カスタマ網を接続できるという意義は大である。

【図面の簡単な説明】

【図1】本発明の基本構成を示すシステムブロック図である。

【図2】本発明の実施例を示すシステムブロック図である。

【図3】本発明のエッジノードの機能を示す概略図である。

【図4】エッジノードにおけるVRテーブルとプロバイダ網側インタフェースとの関係を示す概念図である。

【図5】VRテーブルの内容の一例を示す図である。

【図6】VRテーブルの内容の一例を示す図である。

【図7】VRテーブルの内容の一例を示す図である。

【図8】本発明の実施例の動作を説明するためのシーケンス図である。

【図9】本発明の実施例におけるパケット転送時の動作を示すフローである。

【図10】カプセル化及び逆カプセル化を説明するための図である。

【図11】本発明の実施例におけるカプセル受信時の動作を示すフローである。

【図12】本発明の実施例における制御パケット受信時の動作を示すフローである。

【図13】本発明の実施例における現用リンク障害時の動作を示すフローである。

【図14】本発明の実施例における予備リンクアクティブ時の動作を示すフローである。

【図15】本発明の他の実施例の概略システムブロック図である。

【図16】従来技術を説明するための概略システムブロック図である。

【符号の説明】

A1～A3 カスタマ網

C1 プロバイダ網

1 終端部

2 制御部

3 VRテーブル

4 ROM

5, 6 インタフェース部

11～13, 221～23,

31～33 カスタマノード

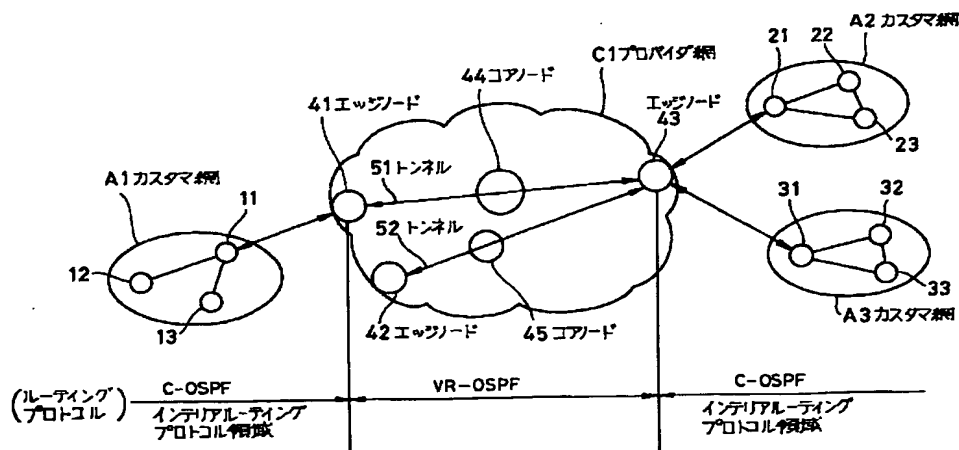
41～43 エッジノード

51 現用トンネル

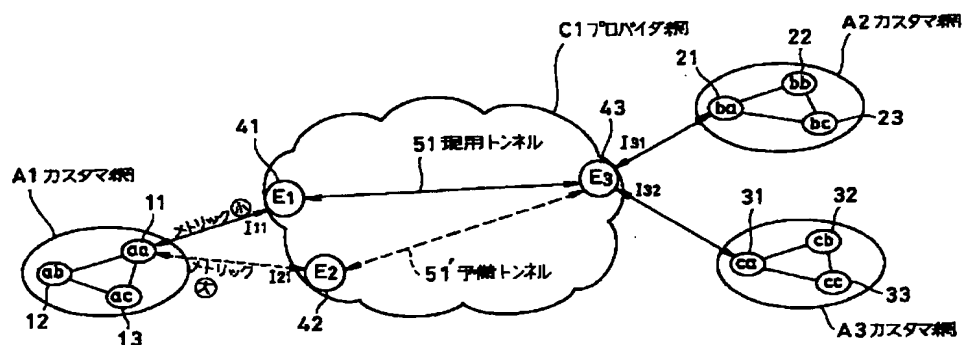
51' 予備トンネル

100 集中処理装置

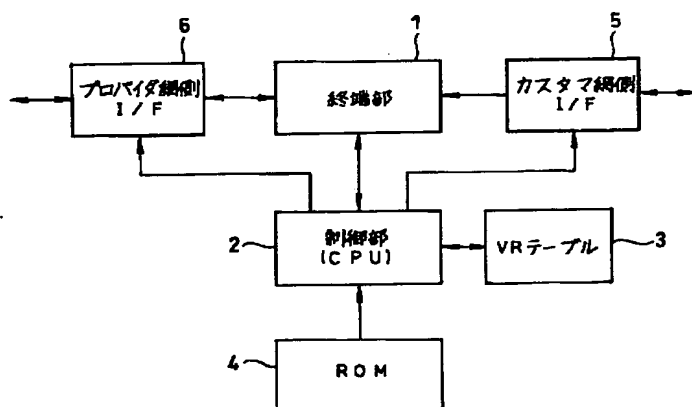
【図1】



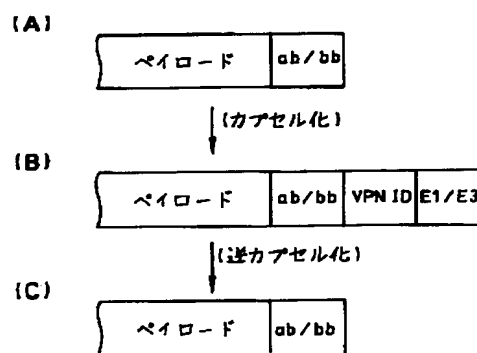
【図2】



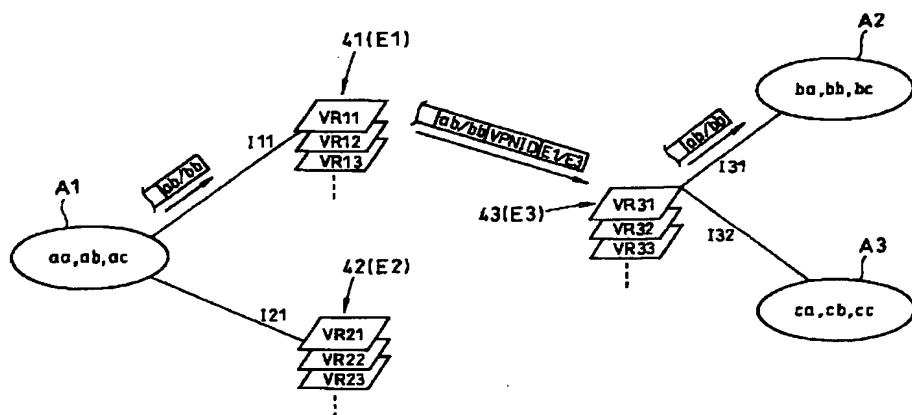
【図3】



【図10】



【図4】



【図5】

41(E1)のVRテーブル

VR テーブル ID	カスタマ側 INF	VPN ID	宛先 プライベート アドレス	カプセル化 アドレス	Egress エッジ のカスタマ側 INF状態	VRからの 出力INF	カプセル化 アドレスの 優先度
11	111	1	aa	—	—	111	—
			ab	—	—	111	—
			ac	—	—	111	—
			ba	E 3	OK/NG	プロバイダ側	1
			bb	E 3	OK/NG	プロバイダ側	1
			bc	E 3	OK/NG	プロバイダ側	1
			ca	E 3	OK/NG	プロバイダ側	1
			cb	E 3	OK/NG	プロバイダ側	1
			cc	E 3	OK/NG	プロバイダ側	1

【図6】

42(E2)のVRテーブル

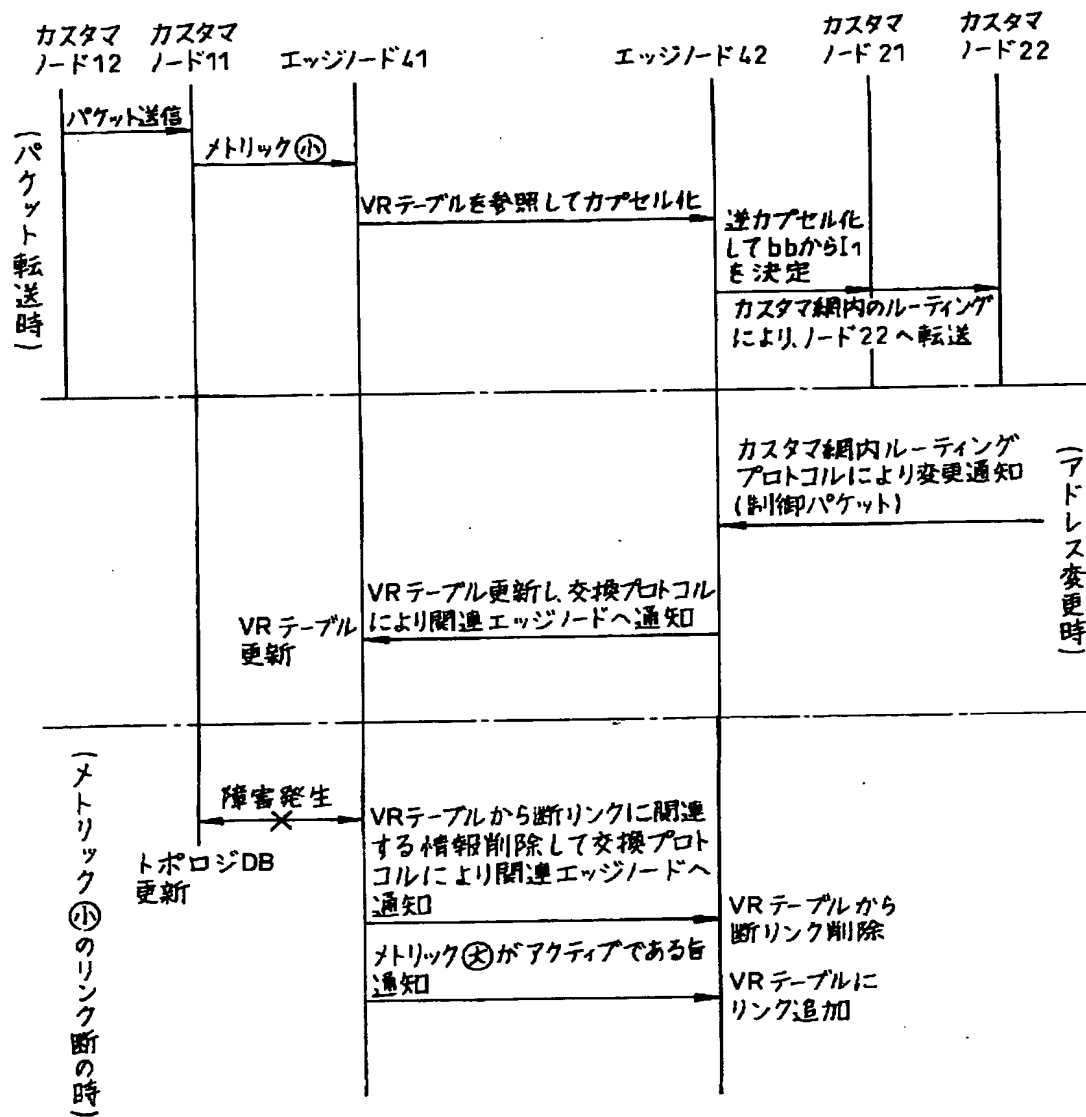
VR テーブル ID	カスタマ側 INF	VPN ID	宛先 プライベート アドレス	カプセル化 アドレス	Egress エッジ のカスタマ側 INF状態	VRからの 出力INF	カプセル化 アドレスの 優先度
21	121	1	aa	—	—	121	—
			ab	—	—	121	—
			ac	—	—	121	—
			ba	E 3	OK/NG	プロバイダ側	1
			bb	E 3	OK/NG	プロバイダ側	1
			bc	E 3	OK/NG	プロバイダ側	1
			ca	E 3	OK/NG	プロバイダ側	1
			cb	E 3	OK/NG	プロバイダ側	1
			cc	E 3	OK/NG	プロバイダ側	1

【図7】

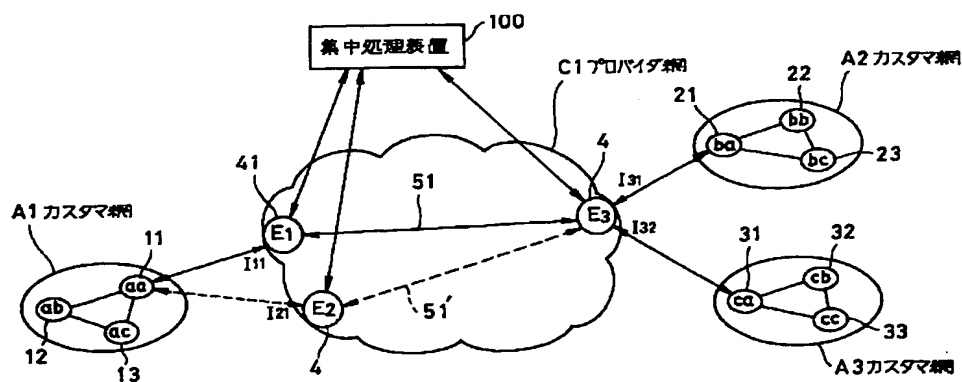
43(E3)のVRテーブル

VR テーブル ID	カスタマ側 INF	VPN ID	宛先 プライベート アドレス	カプセル化 アドレス	Egress エッジ のカスタマ側 INF 状態	VR からの 出力 INF	カプセル化 アドレスの 優先度	
31	131	1	a a	E 1	OK / NG	プロバイダ側	1	
				E 2	OK / NG	プロバイダ側	2	
			a b	E 1	OK / NG	プロバイダ側	1	
				E 2	OK / NG	プロバイダ側	2	
			a c	E 1	OK / NG	プロバイダ側	1	
				E 2	OK / NG	プロバイダ側	2	
	132		b a	—	—	131	—	
			b b	—	—	131	—	
			b c	—	—	131	—	
			c a	—	—	132	—	
			c b	—	—	132	—	
			c c	—	—	132	—	

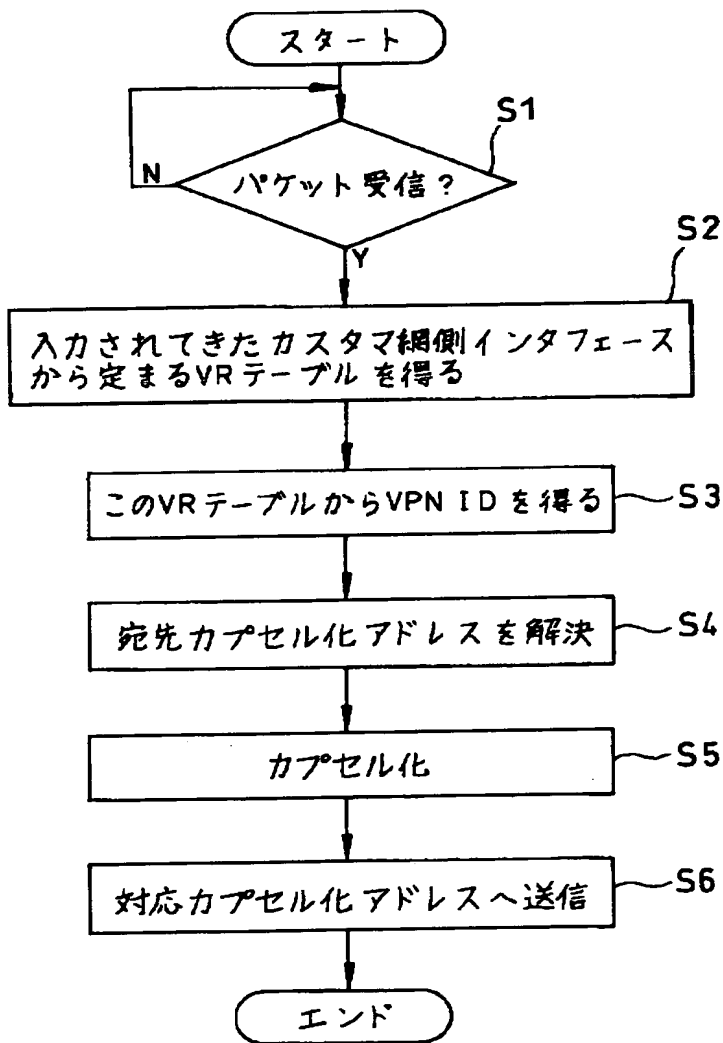
【図8】



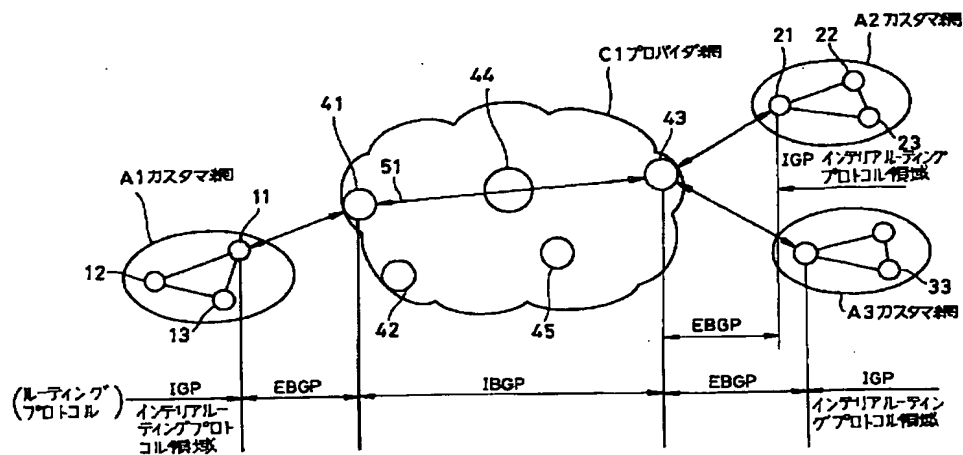
【図15】



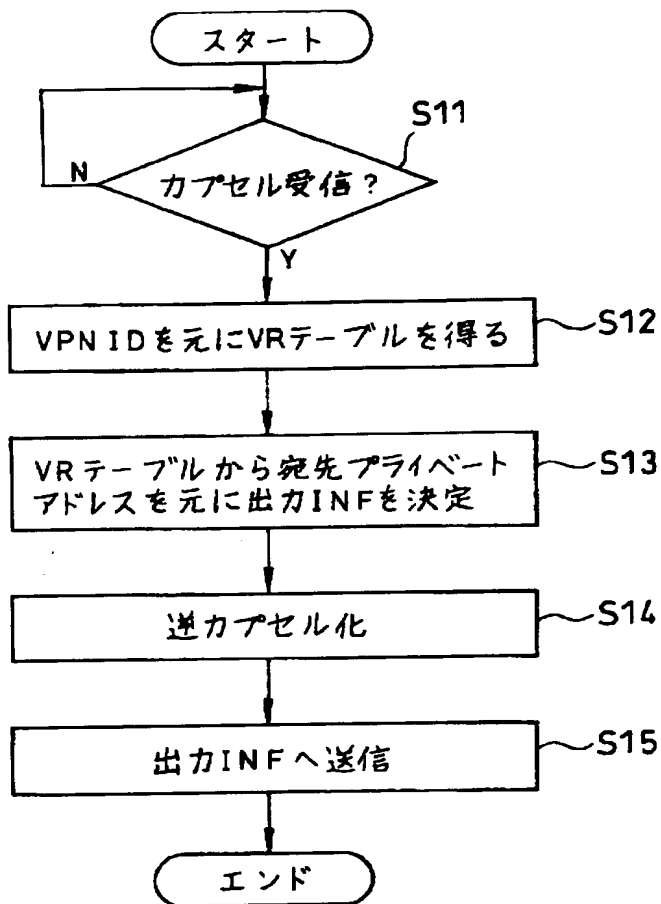
【図9】



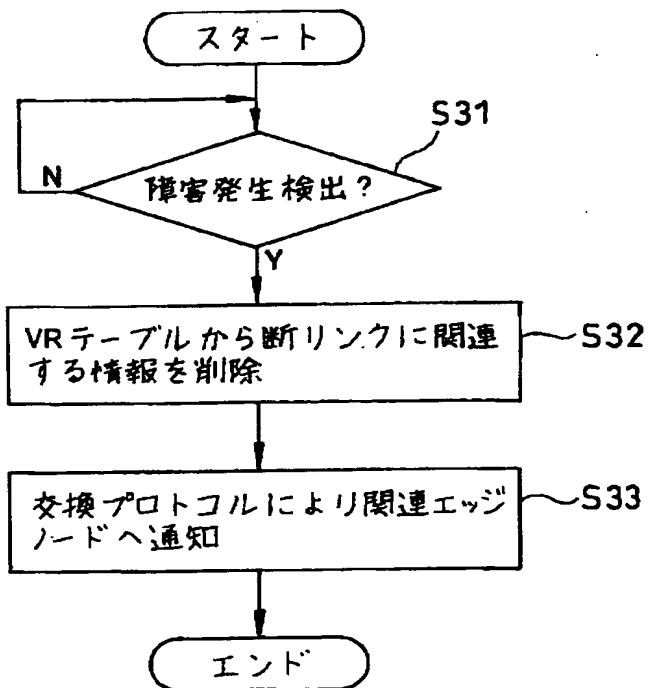
【図16】



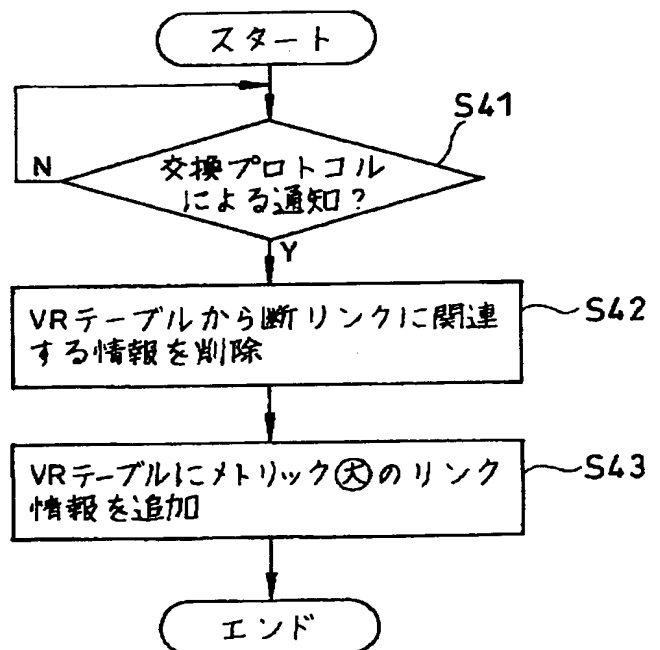
【図11】



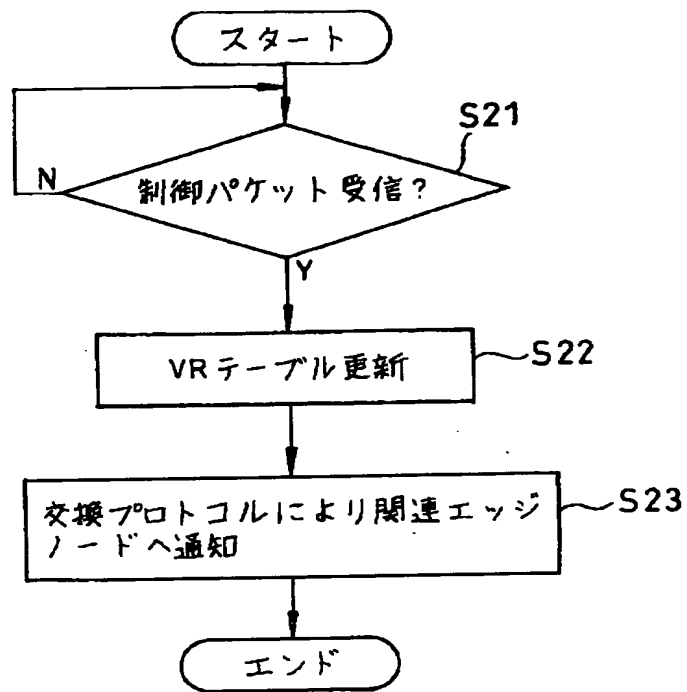
【図13】



【図14】



【図12】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.